WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Carol Davis, Plaintiff, v. HDR Incorporated, Defendant.	No. CV-21-01903-PHX-ROS **ORDER**

In her First Amended Complaint, Plaintiff Carol Davis alleges Defendant HDR Incorporated unlawfully collected electronic communications of private Facebook groups in violation of the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq.*, the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, and the common law right to privacy. (Doc. 18). Defendant moved to dismiss Plaintiff's original complaint based primarily on the fact that the communications Plaintiff alleges Defendant collected were not private, but instead were "readily accessible to the public." The Court agreed and dismissed Plaintiff's complaint with leave to amend. Plaintiff amended her complaint, but Defendant now argues Plaintiff failed to remedy that basic flaw. For the reasons below, the Court agrees, and the Motion to Dismiss will be granted.

I. BACKGROUND

The factual background in this case is set forth in detail in the previous Order. *See Davis v. HDR Incorporated*, --- F. Supp. 3d ---, 2022 WL 2063231, *1 (D. Ariz. June 8, 2022) (summarizing facts of this case). The Court briefly recites the facts as alleged in the

First Amended Complaint.

Defendant is an architecture and design firm that has designed over 275 jails and prisons. (Doc. 18 at ¶ 3). Defendant also offers various strategic communications services, including helping clients to "leverage web, video, and social networking" in order to "manage the social and political risk associated with infrastructure development." (Doc. 18 at ¶ 14). These services include "STRATA," a 24/7 surveillance or "social listening service" that gathers social media data in order to "determine trends, specify key influencers and mitigate or identify risk." (Doc. 18 at ¶¶ 17, 24). In other words, Defendant monitors social media accounts in an attempt to anticipate, and potentially frustrate, opposition to its clients' projects.

This case involves two "private" Facebook groups. The first, "Ahwatukee411," is a private Facebook group formed in 2014 with approximately 32,400 members. (Doc. 18 at ¶ 31). Ahwatukee411 is a forum where residents of the Ahwatukee Foothills area can discuss issues concerning the community. (*Id.*) In order to join Ahwatukee411, a prospective member must fill out a questionnaire explaining their involvement in the community and their interest in joining the group. (Doc. 18 at ¶ 32). The second group, Protecting Arizona's Resources & Children (PARC), was formed to protest the construction of a highway that cuts through the Moahdak Do'ag Mountain. (Doc. 18 at ¶ 33). PARC has approximately 930 members. (*Id.*) There is also a "screening process" required to join PARC. (Doc. 18 at ¶ 34).

Plaintiff has been a member of Ahwatukee411 since 2015, and a member of PARC since 2016. (Doc. 18 at ¶¶ 47, 49). She alleges she privately communicated in each of these groups about topics such as recommendations for services and debates over local issues, including the construction of a local highway, potential political corruption, and the environmental impact of the highway. (Doc. 18 at ¶¶ 48, 50). Plaintiff alleges Defendant infiltrated both groups in 2016 and has undertaken tracking, reading, intercepting, and analyzing the posts of Plaintiff and of other group members. (Doc. 18 at ¶ 54). While Plaintiff alleges it "is unknown how Defendant infiltrated these Private Facebook Groups,"

she alleges that based on the questionnaire screening required for both, the "clear inference is that Defendant used deceitful and untruthful answers to the screening process" in order to join. (Doc. 18 at ¶¶ 40-41).

Plaintiff brought suit in November 2021 against Defendant on behalf of herself and two purported classes of members of the Groups. (*See* Doc. 18 at ¶¶ 57-64). The Court granted Defendant's motion to dismiss in June of 2022, and Plaintiff filed her First Amended Complaint that same month. Defendant's motion to dismiss followed.

A. The Court's Reasoning in Dismissing the Initial Complaint

The Federal Wiretap Act and the Stored Communications Act prohibit intercepting or collecting certain electronic communications. However, the statute makes clear "it shall not be unlawful . . . for any person (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g); *Davis*, 2022 WL 2063231, at *3 (quoting 18 U.S.C. § 2511(2)(g)(i)) ("[e]lectronic communications which are 'readily accessible to the general public' are explicitly exempted from protection under the Wiretap Act and the [Stored Communications Act]."). [1] Therefore, to state a plausible claim under either Act, Plaintiff must allege sufficient facts establishing her communications were not, in fact, "readily accessible to the general public." *See Davis*, 2022 WL 2063231, at *4 (citing *Snow*, 450 F.3d at 1321) ("the readily accessible issue concerns a 'material and essential' element of [Wiretap Act and Stored Communications Act] claim[s] that must be sufficiently pleaded to in the complaint.").

In dismissing Plaintiff's original complaint, the Court held Plaintiff failed to plausibly allege facts showing Plaintiff's posts in the two Facebook groups were

[1] The Electronic Communications Privacy Act encompasses both the Wiretap Act and the Stored Communications Act. *Davis*, 2022 WL 2063231, at *3. The Wiretap Act protects communications in transit, while the Stored Communications Act protects stored communications. *Id.* While the interplay of these two statutes is "complex," *see id.* at *3, n.3 (quoting *Konop*, 302 F.3d at 874), for the purposes of this Order, there is a single relevant inquiry. Both statutes exempt electronic communications which are "readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i).

"configured in some way so as to limit ready access by the general public." *Id.*, at *9 (quoting *Snow v. DirecTV*, 450 F.3d 1314, 1322 (11th Cir. 2006)). The Court adopted two interconnected rationales for this conclusion. The first involved the lack of control Plaintiff retained over her communications while the second involved the relatively simple steps anyone could pursue to obtain access to Plaintiff's communications.

The Court's first rationale was Plaintiff did not "actively restrict[] the public from accessing the information," but instead did "just the opposite" by "posting in a place where she had no ability to restrict access." *Id.* at *7 (quoting *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013)). Because the group administrators determined access to the private groups, and not Plaintiff, the Court explained, Plaintiff's posts in the groups were "readily accessible to the general public."

The Court's second rationale was that though the Facebook groups were labeled as "private," they did not require any meaningful effort to join. That is, "*any* person can become a member of the Groups, provided that they assert some unspecified level of involvement and interest in the community." *Id.*, at *5. The ease by which someone could join the groups meant the groups were "readily accessible to the public."

In adopting these rationales, the Court noted the Ninth Circuit had not addressed the question specifically. *Id.* at *3. Thus, the Court reasoned primarily from two cases: *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) and *Snow*, 450 F.3d 1314 (11th Cir. 2006). In *Konop*, the plaintiff created and maintained a restricted website; he created a discrete list of individuals who were eligible to access a website, and he controlled access to his site by requiring users to log in by entering the name of an eligible person and creating a password. 302 F.3d at 872. After the defendant gained access to the website by impersonating an authorized individual, the plaintiff sued. The Ninth Circuit did not address the requirement that the communications not be readily accessible to the public, but implicit in the *Konop* opinion's analysis is the conclusion that the website at issue was sufficiently private such that it was not readily accessible to the public.

The Court concluded *Konop* did not apply to this case because of materially

different facts. In particular, Plaintiff did not control access to her communications, but the administrators of the private groups did; additionally, the list of eligible users in *Konop* was itself non-public, whereas here, the information required to join Ahwatukee411 and PARC was in the public domain.

Instead of analogizing to *Konop*, the Court explained the facts alleged in the original complaint were more analogous to those in *Snow*. *Davis*, 2022 WL 2063231, at *6. In *Snow*, the plaintiff maintained an electronic bulletin board regarding his contentious dealings with DirecTV. The plaintiff's bulletin board allowed anyone to use the site by registering and creating a password, as long as the registrant clicked a button to agree to the terms of use and to "affirm his non-association with DirecTV." 450 F.3d at 1321. After DirecTV accessed the website, the plaintiff sued under the Stored Communications Act. The Eleventh Circuit concluded the Stored Communications Act did not apply because "[n]othing inherent in any of [the steps required to access the website] prompts us to infer that access by the general public was restricted." *Id*. at 1321-1322. Rather, the Eleventh Circuit found the website's admission requirement to be "in essence, a self-screening methodology by which those who are not the website's intended users would voluntarily excuse themselves." *Id.* at 1322.

Tracking the reasoning in *Snow*, the Court in this case reasoned Plaintiff's allegations about the private Facebook groups established they operated on a similar "self-screening" requirement, because anyone could become a member of the private groups "provided that they assert some unspecified level of involvement and interest in the community." *Davis*, 2022 WL 2063231, at *5. The Court further explained that those who lack involvement or interest in the Ahwatukee community are unlikely to seek admission in the group, but even so, the information required to be admitted to the group is publicly available. *Davis*, 2022 WL 2063231, at *5.

Accordingly, the Court dismissed Plaintiff's claims under the Wiretap Act and the Stored Communications Act (Counts I-III) because she failed to plausibly allege that her posts were not readily accessible by the general public. *Id.* at *9. The Court granted leave

to amend but did not specify the type of additional allegations that might be sufficient to state claims.

B. First Amended Complaint: Private Facebook Groups

To frame the current discussion, the Court begins by reciting in detail the facts about the two private Facebook groups as alleged by Plaintiff in her First Amended Complaint. Some of these facts were in the previous complaint while some of them were added when Plaintiff amended.

Facebook allows users to create and join two different types of groups: private and public. (Doc. 18 at ¶ 25). In private groups, only members can see the identity of other group members and what they post within the group. (*Id.*) Once a private group is created, the group administrators cannot change the group to "public." (Doc. 18 at ¶ 26). The only change the administrators can make is to allow the group to be searchable by non-members (i.e., visible) or not (i.e., hidden). (*Id.*) Members of a private Facebook group can access the names of all the other members within the group, and they can also see when the number of members increases or decreases. (Doc. 18 at ¶ 27). Plaintiff alleges "a member of a private Facebook group could investigate the names of group members and determine whether he or she feels comfortable continuing to post in the private Facebook group in light of the current membership." (*Id.*)

As mentioned above, both groups relevant to this litigation are private Facebook Groups; Ahwatukee411 has about 32,400 members, and PARC has about 930 members. (Doc. 18 at ¶¶ 31, 33). Plaintiff alleges prospective members of Ahwatukee411 must fill out a questionnaire "discussing their involvement in the Ahwatukee community and their interest in joining the group as it relates to the community." (Doc. 18 at ¶ 32). Plaintiff alleges prospective members of PARC must similarly "undergo a screening process." (Doc. 18 at ¶ 34). Plaintiff asserts the purpose of keeping both groups private is to "ensure that only residents" (in the case of Ahwatukee411) or "largely only residents" (in the case of PARC) are able to join the group and see the posts. (Doc. 18 at ¶¶ 32, 34).

Plaintiff alleges the screening process required to join these two private Facebook

groups is "more sophisticated than simply clicking a button to state they are interested in joining." (Doc. 18 at ¶ 36). According to Plaintiff, while all of the information needed to gain admission to the private groups is public, prospective members would need to devote resources and time to gathering the information needed to pass the screening process. (Doc. 18 at ¶ 37). Plaintiff alleges the questionnaire requires: (i) knowing about and researching "the existence of the Ahwatukee community and the issues surrounding the community"; (ii) having "substantial knowledge" of issues facing the community, including construction of the highway, and (iii) drafting "answers to the screening questions discussing the prospective member's interest in the community based on" that research, "as well as stating where the prospective group member resides." (Doc. 18 at ¶ 36). Plaintiff alleges gathering this information is "not something a member of the 'general public' would ever do in practice," and that only a true member of the Ahwatukee community or a "sophisticated social media listening company that specializes in exactly this type of research" would do so. (Doc. 18 at ¶ 37).

Plaintiff does not allege any additional facts, such as the questions required by the questionnaire or the number, if any, of applications to join the group that were denied based on insufficient questionnaire answers. Plaintiff does, however, allege "the clear inference is that Defendant used deceitful and untruthful answers to the screening process" in order to gain membership. (Doc. 18 at ¶ 41). Plaintiff alleges that if Defendant had been truthful in its answers, it would not have been admitted to the private groups, or that even if the administrators did admit Defendant upon reading its truthful answers, she and other members would have seen that Defendant had been added to the group and could have investigated Defendant and potentially opted not to post anymore. (Doc. 18 at ¶ 42). Plaintiff instead alleges she did not know, nor "have reason to know, that her communications were being surveilled by unconsented-to third-party actors who were neither Ahwatukee residents nor persons whose interests were not aligned with the PARC organization's goals." (Doc. 18 at ¶ 53).

//

II. LEGAL STANDARD

Pursuant to Rule 12(b)(6), a complaint may be dismissed for failure to state a claim for which relief can be granted. Fed. R. Civ. P. 12(b)(6). "[A] complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "The purpose of a motion to dismiss under Rule 12(b)(6) is to test the legal sufficiency of the complaint." *N. Star Int'l v. Ariz. Corp. Comm'n*, 720 F.2d 578 581 (9th Cir. 1983). A claim is facially plausible when it contains "factual content that allows the court to draw the reasonable inference" that the moving party is liable. *Ashcroft*, 556 U.S. at 678, 129 S. Ct. 1937. In reviewing a motion to dismiss, the Court takes "all allegations of material fact as true and construe[s] them in the light most favorable to the non-moving party." *Parks Sch. of Bus. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995). A complaint does not suffice "if it tenders 'naked assertion[s]' devoid of 'further factual enhancement.'" *Ashcroft*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 557)).

III. ANALYSIS

A. Claims under the Federal Wiretap Act and the Stored Communications Act (Counts I-III)

Other than the previous Order in this case, there is no case directly on point. However, in her response to the pending motion to dismiss, Plaintiff argues the Court's prior Order was inappropriately strict and a better reading of the relevant case law supports the conclusion that the private Facebook groups were not "readily accessible to the general public." The Court's rationale that Plaintiff's lack of control over her communications was meaningful was likely an overstatement. However, the Court's view that the Facebook groups effectively were readily accessible to the general public remains accurate.

In attempting to show the Facebook groups were not, in fact, readily accessible to the general public, Plaintiff relies on *Joffe v. Google, Inc.*, 729 F.3d 1262 (9th Cir. 2013). In that case, Google's Street View cars gathered and stored data sent over unencrypted Wi-Fi networks in the houses they drove past. *Id.* at 1264. The Ninth Circuit initially held those

Wi-Fi communications, though unencrypted, were not readily accessible to the general public, because the data was only accessible within a few hundred feet of the Wi-Fi source and "most of the general public lacks the expertise to intercept and decode payload data transmitted over a Wi-Fi network." *Id.* at 1278-79. Plaintiff argues that gathering the information required to pass the questionnaires for admission to the private Facebook groups here is analogous to those sophisticated collection methods used by Google.

However, as Defendant points out, the initial opinion in *Joffe* was amended and superseded on rehearing. *Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013). The superseding opinion did not include this section of analysis at all. Regardless, even under the analysis and facts of the first *Joffe* opinion, Plaintiff's argument overstates the similarities. To gain admission to the private Facebook groups, prospective members must fill out a questionnaire; Plaintiff admits in her First Amended Complaint that all of the information required for the questionnaires is publicly available. (Doc. 18 at ¶ 37). Plaintiff alleges that the "time, effort, and knowledge one would have to accrue or devote to research to pass the screening process" means a member of the general public would never, in practice, undertake the process. (*Id.*) But conducting some basic online research is not the same in degree or in kind as the type of "sophisticated hardware and software" combined with geographic proximity that Google utilized in *Joffe*.

Plaintiff's additional case law analyzes confidentiality and privacy under other statutes. For example, in a breach of confidentiality case, *Tori Belle Cosmetics, LLC v. Meek*, No. 21-0066, 2022 WL 670923 (W.D. Wa. Mar. 7, 2022), the plaintiff alleged the defendants used confidential trade secrets, including training materials, customer and contact lists, plans, and financials to create a competing cosmetic line. *Id.* at *5. The defendants argued the materials were not kept in confidence, because they were posted to a private Facebook group with thousands of members. *Id.* The court agreed with the plaintiff, finding that the private Facebook group at issue was only used for training, was only open to Tori Belle affiliates, and that each affiliate had to agree to keep the material shared in the group confidential. *Id.*

Unfortunately, the decision does not explain how individuals were admitted to the group or the ease by which a member of the general public might impersonate someone and gain access. But the Plaintiff's allegations are sufficiently different from *Tori Belle Cosmetics*. Here, the private group was not limited to affiliates of a certain corporation or entity, but to anyone with a self-identified interest in the Ahwatukee community; Plaintiff did not allege that there was any agreement to maintain confidentiality or privacy among the members or between the members and the administrators; and Plaintiff did not control or oversee access to the private groups.

The Plaintiff next cites *Greenburg v. Wray*, No. CV-22-00122-PHX-DLR, 2022 WL 2176499 (D. Ariz. June 16, 2022). In that case, brought under the Computer Fraud and Abuse Act, the plaintiff alleged the defendants found a URL to plaintiff's Google Drive and publicly disclosed its contents. *Id.* at *1. The Google Drive was not password protected, but it was not indexed to be searchable by any search engine, so it was only available to anyone who could type in the exact 68-character URL. *Id.* at *2. The Court found it was a "close call," but denied the motion to dismiss and found that the Google Drive was sufficiently private to state a claim under that statute. The Drive was not password protected; however, the fact that the Drive was not searchable, so someone would need the exact 68-character URL to access it, made it plausible that the Drive was not "readily accessible" to the general public.[2] *But see* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1164–65 (2016) ("A hard-to-guess URL is still a URL, and the information posted at that address is still posted and accessible to the world."). Importantly, here, Defendant (or any prospective member of the two private groups) did not need any information that was not readily publicly available, like a long URL, *see Greenburg*, 2022 WL 2176499, at *2, or a name from a private list, *see Konop*, 302 F.3d at 872. Instead, prospective members needed only to indicate their interest in the

[2] Here, it is worth noting, while Plaintiff alleges the two groups at issue here are private, she does not allege whether or not they were "hidden" (i.e., not searchable by the general public) or "visible" (i.e., indexed and searchable). (*See* Doc. 18 at ¶ 26). There is a difference between finding and exploiting an inadvertently revealed 68-character URL and searching for "Ahwatukee" on Google or Facebook and seeking entrance to a private group that pops up as a result.

Ahwatukee community and the issues affecting the community, all of which was easily and publicly available. (Doc. 18 at ¶ 36-37).

Plaintiff points to *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022), a case the Ninth Circuit considered under the Computer Fraud and Abuse Act ("CFAA"), a statute very similar to the Stored Communications Act. *Id.* at 1200. In that case, the plaintiff alleged the defendant had violated CFAA by "scraping" information that users included on their individual, publicly accessible LinkedIn profiles. *Id.* at 1187. The relevant question was whether that "scraping" constituted accessing LinkedIn's computers "without authorization." *Id.* at 1195. The Ninth Circuit's discussion of that question contains broad language that Plaintiff point to in support of her claims.

According to the Ninth Circuit, the CFAA should be viewed as an "anti-intrusion statute," because it targets conduct "analogous to 'breaking and entering.'" *Id.* at 1197. Thus, liability under the "CFAA is premised on a distinction between information presumptively accessible to the general public and information for which authorization is generally required." *Id.* at 1199-1200. The Ninth Circuit held the CFAA only addresses the latter. That understanding was described as "consistent" with the Ninth Circuit's interpretation of the Stored Communications Act. In particular, the Stored Communications Act distinguishes "between public websites and non-public or 'restricted' websites, such as websites that are password-protected . . . or require the user to purchase access by entering a credit card number." *Id.* at 1200. The legislative history of the Stored Communications Act indicates "[a] person may reasonably conclude that a communication is readily accessible to the general public if the . . . means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." *Id.* Communications where there is an attempt to retain privacy "would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public." *Id.*

Plaintiff points to this broad language and emphasizes the role of the restrictions in the private Facebook groups. But the present complaint fails to include sufficient facts

regarding the type of authentication that was required to render Plaintiff's claims plausible. Again, the complaint does not contain the questions that had to be answered, nor does it explain whether the application process was meaningful in that applicants were routinely denied. Put in the language of *hiQ Labs*, the "means of access" may have been "widely known." Plaintiff alleges the information required by the questionnaires was so detailed that no "member of the 'general public' would ever" gather that information. (Doc. 18 at 11). But no details regarding that information is provided. In addition, while the number of members of the groups is not dispositive, the fact that over 32,400 individuals were members of one of the groups indicates it may have been simple to join.

It is undisputed that these private Facebook groups had at least some "indicia of intended privacy," because they were identified as "private" and required permission to become a member. Moreover, if Plaintiff is correct and Defendant knowingly falsified information to gain access to the groups, Defendant must have known it was on thin ice by obtaining access to information under false pretenses. At least with respect to the much smaller PARC group, it appears to be plausible that requiring a questionnaire is sufficient indication that it was limited to a select few, and there were attempts to retain confidentiality. However, Plaintiff's new allegations are not enough to create plausible claims for relief.

Plaintiff raises a smattering of other arguments regarding the private nature of Facebook groups, none of which is persuasive. The Court does not find much significance in Plaintiff's repeated assertion that once a Facebook group is created as "private," it can never be transformed to be "public." (Doc. 18 at ¶ 26). The nominal designation of the group does not determine whether the communications are readily accessible to the general public. Indeed, the administrators of these two private groups could presumably change the entry criteria; for example, they could make the requirements much more stringent, or they could reduce them to a check box reminiscent of the facts in *Snow*. *See* 450 F.3d at 1321. Plaintiff urges the Court to consider only the privacy status of the groups at the time of her postings, not the risk that such status may change; however, the legal question is not what

her expectation of privacy was when posting, but rather, whether her communications were, in fact, "readily accessible to the public." *See In re Innovatio IP Ventures, LLC Patent Litig.*, 886 F. Supp. 2d 888, 894 (N.D. Ill. 2012) ("the public's expectation of privacy in a particular communication is irrelevant to the application of the Wiretap Act as currently written.").[3] Plaintiff may have wanted her posts to be seen only by the members of these two private groups (32,400 members of Ahwatukee411 and 930 of PARC); but that is irrelevant to the question of whether her posts were, in fact, readily accessible to the general public.

Plaintiff also points the Court to a recent FTC Settlement with Facebook, under which Facebook was prohibited from disclosing "nonpublic user information" to third parties without meeting certain requirements not relevant here. (Doc. 18 at ¶ 30). The FTC defined "nonpublic user information" as "any user profile information . . . or user-generated content . . . that is restricted by one or more Privacy Setting(s)." (*Id.*) Plaintiff argues her posts were "nonpublic user information" under this definition and urges the Court to import that definition to the analysis here. However, as an initial matter, the FTC Settlement terms are irrelevant to the question of whether Plaintiff's communications were readily accessible to the general public.[4] Moreover, the FTC definition actually serves to highlight the weakness in Plaintiff's allegations: Plaintiff did not allege that she restricted any of her content to certain users (for example, through any of her own privacy settings), but instead alleged that she posted in a group with a membership she did not control or oversee—a membership which could (and did) change without her permission or knowledge. *See Ehling*, 961 F. Supp. 2d at 668 ("Cases interpreting the [Wiretap Act and Stored Communications Act] confirm that information is protectable as long as the communicator actively restricts the public from accessing the information."). While the

[3] The statute does include an analysis of the speaker's expectation of privacy when an oral communication is at issue. 18 U.S.C. § 2510(2). However, "there is no comparable requirement for electronic communications." *Lane v. Brocq*, No. 15-C-6177, 2016 WL 1271051, at *7 (N.D. Ill. Mar. 28, 2016) (citing 18 U.S.C. § 2510(12)).

[4] Additionally, while it may be true that Defendant's conduct violated Facebook's terms and policies against scraping data, that likewise does not necessarily impact whether or not Plaintiff's posts were "readily accessible to the general public."

number of users who can access the information may not be dispositive, *see id.*, it is at least relevant that Plaintiff purposefully posted her content to a group with over 32,400 members in one case and over 930 in another. *See Margolies v. Rudolph*, No. 21-CV-2447-SJB, 2022 WL 2062460, at *7 (E.D.N.Y. June 6, 2022) (a private Facebook group with over 14,000 members "has the character of 'a place open to the public,' because it has no meaningful barriers to entry—to join one need only agree to the rules of the group—and its members appear to be free to speak online about any subject openly").[5]

Accepting as true all the facts alleged by Plaintiff in her First Amended Complaint, a question of the extent of privacy is raised. On the one hand, the Facebook groups were nominally private and had entry requirements that included a questionnaire asking for detailed information about the prospective member's interest in the community. On the other hand, Plaintiff had no control over whom the administrators allowed into the groups, or whether they would change their entrance criteria at any point to be more or less stringent. The groups had vast membership (over 32,400 members in Ahwatukee411, and over 930 in PARC). And while the questionnaire, as alleged, presented a higher barrier to entry here than there was in *Snow* (which required acknowledging a potential member had no affiliation with DirecTV) or *Margolies* (which required agreeing to the rules of the group), the current allegations appear to show that anyone, anywhere, with an internet connection and an interest in the community, could join the groups, unlike the non-public communications in *Konop* and *Tori-Belle Cosmetics*.

For these reasons, Plaintiff has failed to plausibly allege that her electronic communications posted into the private Facebook groups were not readily accessible by the general public. Accordingly, Plaintiff's claims under the Wiretap Act and the Stored Communications Act (Claims I-III) will be dismissed with one final opportunity to amend. Should Plaintiff choose to amend, she should allege the information that was elicited by the questionnaires and, if possible, whether any individuals were denied entry after filling

[5] *Margolies* did not arise under the Wiretap Act or Stored Communications Act but was analyzing a Facebook group in the context of a defamation claim. 2022 WL 2062460, at *4-7.

out the questionnaires.

B. Invasion of Privacy Claim (Count IV)

Plaintiff's fourth claim is for common law invasion of privacy or intrusion on seclusion. (Doc. 18 at ¶¶ 96-107). A claim for intrusion upon seclusion or invasion of privacy requires the Plaintiff to prove: (i) an intentional intrusion, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns; and (ii) that the intrusion would be highly offensive to a reasonable person. *Hart v. Seven Resorts, Inc.*, 190 Ariz. 272, 279 (Ct. App. 1997) (citing Restatement (Second) of Torts § 652B). The first element requires "(a) an actual, subjective expectation of seclusion or solitude in the place, conversation, or matter, and (b) that the expectation was objectively reasonable." *Med. Lab'y Mgmt. Consultants v. Am. Broad. Cos., Inc.*, 306 F.3d 806, 812 (9th Cir. 2002).

Plaintiff alleges she had a subjective expectation of privacy in her posts in the private groups. (Doc. 18 at ¶¶ 99, 102). She alleges she believed the posts would only be seen by other (genuine) members of the private groups, not by a company pretending to be such a member. (*See id.*) Regardless of her subjective expectation, the Court has little trouble concluding that any such expectation was not objectively reasonable. As an initial matter, as discussed extensively above, Plaintiff herself has not alleged that she took any steps to maintain "a private seclusion" around her "person or affairs." Restatement (Second) of Torts § 652B cmt. c (1977). Rather, she posted her communications in a Facebook group of over 32,400 people and in another group of over 930 people, both of which were administered by third parties she did not control or oversee. Plaintiff argues her expectation of privacy was reasonable because: (i) the groups were designated as "private" and required filling out a questionnaire to be admitted; (ii) the FTC settlement's definition of "nonpublic user information" arguably covers the private groups; and (iii) and Defendant's alleged conduct violated Facebook's terms and conditions. None of those factors, nor all three combined, however, renders her expectation of privacy in these groups objectively reasonable. Indeed, Plaintiff's first amended complaint acknowledges that Facebook's Frequently Asked Questions includes a warning that "[u]nauthorized scraping

is often done in a way that disguises the activity so that it blends in with ordinary usage." (Doc. 18 at ¶ 29). That could be read as a statement that Plaintiff should have expected "scraping" and further distribution of her posts. Thus, if anything, Plaintiff and other users should have been on notice that posting in a group with a large membership, even if nominally identified as private, was not a sphere of seclusion, but instead a forum where hundreds or thousands of people could interact based on entry criteria set by a third party that could change at any time. These private groups were not places of seclusion "thrown about" or maintained by Plaintiff. *See id. Compare* Restatement (Second) of Torts § 652B cmt. b (1977) (listing examples of intrusion on seclusion, such as looking into one's window with binoculars, tapping telephone wires, opening private mail, searching his safe or wallet, examining his private bank account, etc.).

Thus, this claim must also be dismissed. And it appears unlikely Plaintiff will able to allege additional facts that would render her expectation of privacy was objectively reasonable. However, in an abundance of caution the Court will allow Plaintiff to amend this claim as well.

IV. CONCLUSION

For the reasons above, the Court finds Plaintiff's claims under the Federal Wiretap Act and the Stored Communications Act must be dismissed. The communications in the two private Facebook groups here were not protected by those statutes. Additionally, Plaintiff's claim for invasion of privacy must also be dismissed.

Accordingly,

…

…

…

…

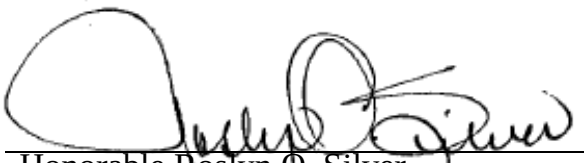
…

…

…

IT IS ORDERED Defendant's motion to dismiss (Doc. 20) is **GRANTED**. Plaintiff's claims are **DISMISSED WITH LEAVE TO AMEND**. Plaintiff shall file an amended complaint no later than thirty days from this order. The Clerk of Court is directed to enter judgment in favor of Defendant if no amended complaint is filed by that date.

Dated this 24th day of January, 2023.



Honorable Roslyn O. Silver
Senior United States District Judge